HowTo

Einrichtung & Konfiguration

Avira AntiVir WebGate (Suite)

Avira Support

Oktober 2009

Inhaltsverzeichnis

1 In welchen Umgebungen kann es eingesetzt werden? *2*

2 Installation *2*

3 Empfohlene Basiskonfiguration *3*

4 Was kann zusätzlich konfiguriert werden? *4*

4.1 Proxyeinstellungen **4**

4.2 Aktiviere ICAP Server **4**

4.3 Erlaube HTTPS Tunnel **4**

4.4 Fortschrittsanzeige **5**

4.5 X-Header **5**

4.6 Zugriffsberechtigter Adressraum **5**

5 Besonderheiten *6*

5.1 Squid als Proxyserver **6**

5.2 ICAP Konfiguration **6**

6 Updatekonfiguration *7*

6.1 Sinnvolle Werte für ein Update **7**

6.2 Große Unternehmen: **7**

6.3 Small Business: **7**

6.4 Kunden mit Schmalband Anschlüssen (Modem/ISDN): **8**

6.5 Internet Service Provider **8**

7 WebGate Suite Features *9*

1 In welchen Umgebungen kann es eingesetzt werden?

- Als Proxyserver mit HTTP sowie FTP over HTTP Überwachung

- Kann sowohl vor als auch hinter einem weiteren Proxyserver fungieren

- Als Integration in eine ICAP (Internet Content Adaptation Protocol) Umgebung

- Als Zugangskontrolle auf Basis von Client IP-Adresse oder Zielport

2 Installation

- Dekomprimieren: gzip -d antivir-webgate-prof.tgz

- Entpacken tar -xvf antivir-webgate-prof.tgz

- Verzeichnis wechseln: cd antivir-webgate-prof.tgz

- Installation ausführen: ./install

Installationsdialog folgen ...

Folgende Abfragen sind empfohlen und sollten übernommen werden:

- Would you like to setup Engine and Signature updates as cron task ? [y]

- Please specify the interval to check. Recommended values are daily or 2 hours.
available options: d [2]

- Please specify if boot scripts should be set up.
Set up boot scripts [y]

3 Empfohlene Basiskonfiguration

HTTP Port
HTTPPort 8080
Dies lässt WebGate auf dem Port 8080 auf Anfragen lauschen. Sofern hier bereits ein anderer Proxyserverdienst läuft, muss dieser Port entsprechend geändert werden.

FTP Port
FTPPort 2121
Auf Wunsch bietet WebGate auch einen FTP Proxydienst.
Sofern hier bereits ein anderer Proxyserverdienst läuft, muss dieser Port entsprechend geändert werden.

Quarantäneverzeichnis
MoveConcerningFilesTo /home/quarantine
#Bei einem Fund wird die Datei in das Quarantäneverzeichnis verschoben und umbenannt. Dadurch ist die Datei zum einen für den User nicht mehr zugänglich, wird aber auch nicht z.B. im Falle eines False Positive gelöscht oder verändert.

Logdatei festlegen
LogFile /var/log/avwebgate.log
Legt die Logdatei des OnAccess-Scanners fest. Standardmäßig wird in das Syslog geschrieben.

Qualität der Ausgabe definieren
LogLevel 4
Dies setzt einen mittleren LogLevel. Es protokolliert Alarme (z.B. Virenfund), Errormeldungen (z.B. Fehlerhafte ACL Konfiguration) und Warnungen (z.B. im Falle eines verschlüsselten Archives)

Aktiviert Heuristik auf Stufe Mittel
HeuristicsLevel 2
Ein guter Mix zwischen Erkennung und Früherkennung. Dies verhindert eine Vielzahl möglicher False Positives.

Aktiviert Erkennung von möglichen Macroviren in Office-Dokumenten
HeuristicsMacro yes
Wir empfehlen den Scan in Office-Dokumenten für eine bestmögliche Überwachung

4 Was kann zusätzlich konfiguriert werden?

Diese Einstellungen sollten vorher bedacht und nur optional bei Bedarf eingetragen werden! Die Werte müssen entsprechend angepasst werden.

4.1 Proxyeinstellungen

Die folgenden Proxyeinstellungen sind ggf. nötig um einen entsprechenden Proxyserver vor WebGate zu schalten.

HTTPProxyServer your.proxy

HTTPProxyPort 3128

HTTPProxyUsername username

HTTPProxyPassword password

FTPProxyServer your.proxy

FTPProxyPort 2121

4.2 Aktiviere ICAP Server

Dies aktiviert den ICAP Server von WebGate. Der Dienst läuft dann zusätzlich auf dem gewählten Port. Der ICAP Server unterstützt sowohl reqmod (Request modification) als auch respmod (Response modification).

Squid unterstützt ICAP 1.0 erst mit der Version 3.x!
ICAPPort 1344

4.3 Erlaube HTTPS Tunnel

WebGate blockt standardmäßig den HTTPS Datenstrom aufgrund dessen, dass dieser nicht gescannt werden kann.
#Sofern Sie dennoch HTTPS Seiten tunneln möchten, können Sie den folgenden Parameter setzen:
Der HTTPS Datenstrom wird _NICHT_ gescannt.

AllowHTTPSTunnel 1

4.4 Fortschrittsanzeige

Eine Seite im Browser anzeigen, welche bei größeren Downloads eine Fortschrittsanzeige ausgibt
Zusätzlich muss ein Intervall in Sekunden festgelegt werden (z.B. 3), welche ein Refresh-Kommando an den Browser schickt.
Das Aktivieren und Konfigurieren der Fortschrittsanzeige erfolgt über den einzelnen folgend genannten Parameter:

RefreshInterval 3

4.5 X-Header

Fügt den X-Header des Clients in der Anfrage hinzu, um nachgeschaltete Proxyserver über den tatsächlich anfragenden Client zu informieren.

AddXForwardedForHeader 1

4.6 Zugriffsberechtigter Adressraum

Dies legt die zugriffsberechtigen Clients bzw. Adressräume fest.
Unberechtigte Clients, die auf WebGate zugreifen möchten, werden blockiert

AllowClientAddresses 127.0.0.1 192.168.0.0/16

5 Besonderheiten

5.1 Squid als Proxyserver

Dies sendet alle Anfragen vom Client an Squid durch WebGate. Dies ermöglicht die Nutzung der Squid-Proxyfunktionen.

Benötigte Einstellungen in der squid.conf

cache_peer <WebGateHost> parent <WebGatePort> 0 no-query no-digest default

acl ALL src 0.0.0.0/0.0.0.0

never_direct allow ALL

5.2 ICAP Konfiguration

Durch das Starten des im Punkt 4.2 beschriebenen ICAP Servers kann Squid als ICAP-Client fungieren um Anfragen zu verarbeiten.

Benötigte Einstellungen in der squid.conf

icap_enable on

icap_service service_1 reqmod_precache 0 icap://[WEBGATE_HOST]:1344/reqmod

icap_service service_2 respmod_precache 0
icap://[WEBGATE_HOST]:1344/respmod

icap_class class_1 service_1

icap_class class_2 service_2

icap_access class_1 allow all

icap_access class_2 allow all

6 Updatekonfiguration

Um Ihre AntiVir Installation auf den aktuellen Stand zu halten, werden zwei Arten von Updates bei der Installation eingerichtet:

- Scannerupdate (nur Scanner & Engine & VDF)
- Produktupdate (Guard Programmdateien)

Die Einstellungen für das Update finden Sie nach der Installation in folgender Datei:

/etc/cron.d/avira_updater:

00 */2 * * * root /usr/lib/AntiVir/avupdate --product=Scanner
15 12 * * Tü root /usr/lib/AntiVir/avupdate --product=Guard

6.1 Sinnvolle Werte für ein Update

Je nach Zielgruppe empfehlen wir unseren Kunden mindestens 2-3 mal am Tag, ein Update durchzuführen.

6.2 Große Unternehmen:

Beispiel: jede Stunde

/etc/cron.d/avira_updater:

* */1 * * * root /usr/lib/AntiVir/avupdate --product=Scanner

6.3 Small Business:

Beispiel: alle 3 Stunden

/etc/cron.d/avira_updater:

* */3 * * * root /usr/lib/AntiVir/avupdate --product=Scanner

6.4 Kunden mit Schmalband Anschlüssen (Modem/ISDN):

Beispiel: alle 8 Stunden

/etc/cron.d/avira_updater:

* */8 * * * root /usr/lib/AntiVir/avupdate --product=Scanner

6.5 Internet Service Provider

Für Internet Service Provider empfiehlt es sich natürlich, deutlich öfter nach neuen Signaturen zu schauen. Daher sollte die Frequentierung der Updateaufrufe deutlich höher angelegt sein, z.B. alle 15 Minuten. So ist sichergestellt, dass Sie immer zeitnah die neuesten Signaturen einsetzen.

/etc/cron.d/avira_updater:

*/15 * * * * root /usr/lib/AntiVir/avupdate --product=Scanner

Es gibt darüber hinaus die Möglichkeit, ein reines Engine- und VDF- Update durchzuführen. Die Guard Produktdateien, sowie der zentrale Scannerdienst (SAVAPI) werden dabei nicht mitaktualisiert.

Dies kann im Allgemeinen sehr interessant für Sie sein, wenn Sie Programmupdates als besonders sensitiv betrachten. Dadurch erhalten Sie die Möglichkeit, auf einem separaten Testsystem zunächst einen Audit durchzuführen, bevor Sie die neue Version produktiv einsetzen.

Der Aufruf dafür lautet:

$ /usr/lib/AntiVir/avupdate --product=Signatures

7 WebGate Suite Features

Mit dem WebGate Suite Feature ist es möglich, bestimmte Kategorien von Webseiten zu blockieren.
Dazu gehören u.a. Pornografie, Phishing, Malware und Fraud.

Filterkategorien festlegen:

Numeric Value	Category
0	Pornography
1	Erotic / Sex
2	Swimwear / Lingerie
3	Shopping
4	Auctions / Classified Ads
5	Governmental Organizations
6	Non-Governmental Organizations
7	Cities / Regions / Countries
8	Education

9	Political Parties	
10	Religion	
11	Sects	
12	Illegal Activities	
13	Computer Crime	
14	Political Extreme / Hate / Discrimination	
15	Warez / Hacking / Illegal Software	
16	Violence / Extreme	
17	Gambling / Lottery	
18	Computer Games	
19	Toys	

| 20 | Cinema / Television |

| 21 | Recreational Facilities / Amusement / Theme Parks |

| 22 | Art / Museums / Memorials / Monuments |

| 23 | Music |

| 24 | Literature / Books |

| 25 | Humor / Comics |

| 26 | General News / Newspapers / Magazines |

| 27 | Web Mail |

| 28 | Chat |

| 29 | Newsgroups / Bulletin Boards / Blogs |

| 30 | Mobile Telephony |

| 31 | Digital Postcards |

| 32 | Search Engines / Web Catalogs / Portals |

| 33 | Software / Hardware / Distributors |

| 34 | Communication Services |

| 35 | IT Security / IT Information |

| 36 | Website Translation |

| 37 | Anonymous Proxies |

| 38 | Illegal Drugs |

| 39 | Alcohol |

| 40 | Tobacco |

| 41 | Self-Help / Addiction |

| 42 | Dating / Relationships |

| 43 | Restaurants / Bars |

44	Travel	
45	Fashion / Cosmetics / Jewelry	
46	Sports	
47	Building / Residence / Architecture / Furniture	
48	Nature / Environment / Animals	
49	Personal Homepages	
50	Job Search	
51	Investment Brokers / Stocks	
52	Financial Services / Investment / Insurance	
53	Banking / Home Banking	
54	Vehicles / Transportation	
55	Weapons / Military	

| 56 | Health |

| 57 | Abortion |

| 59 | Spam URLs |

| 60 | Malware |

| 61 | Phishing URLs |

| 62 | Instant Messaging |

Parameter in der /etc/avwebgate.conf

Blockiert Seiten der Kategorien Pornography (0) _BIS_ Swimwear / Lingerie (2) (enthält Erotic / Sex [1])

sowie Illegal Activities (12) _UND_ Political Extreme / Hate / Discrimination (14) _SOWIE_ Phishing URLs (61)

WSBlockCategories 0-2 12 14 61

##

Weitere Informationen und Einstellungsmöglichkeiten von AntiVir WebGate (Suite) finden Sie im MANUAL, Benutzerhandbuch oder in unserer Wissensdatenbank unter http://www1.avira.com/de/support/kbsearch.php.